UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/583,578	03/27/2007	Dennis Vance Pollutro	099011-2113(CTX-624US)	8867

48329 7590 07/19/2011

FOLEY & LARDNER LLP
111 HUNTINGTON AVENUE
26TH FLOOR
BOSTON, MA 02199-7610

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
07/19/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/583,578	POLLUTRO ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13 and 15-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13 and 15-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to amendment filed on 5/11/2011. Claim 14 is cancelled. Claims 1-13 and 15-21 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claim 21 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Currently, claim 21 is drawn to a "computer readable recording medium". The Examiner notes that applicant explains in paragraphs 36 and 46 that the system may be implemented in a number of mediums and that one such medium includes a "computer readable carrier". Furthermore the applicant indicates that that the "computer readable carrier" includes waves. As such the applicant is advised to do the following: a. Remove the recitation of "Further Still, the system may operate from a computer readable carrier (e.g., solid state memory, optical disk, magnetic disk, radio frequency carrier wave, audio frequency carrier wave. etc) that includes computer instructions (e.g., computer program instruction related to the security system) from paragraphs 36 and 46.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van ©mum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969). A timely filed terminal disclaimer in compliance with 37 CFR 1.321 (c) or 1.321 (d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1, 14, 15, and 21 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 15, 18, 22, and 32 of 'U.S. Patent No. 7,644,434 Pollutro(2)) in view of Williams (US Patent Publication No. 2003/0005118). Pollutro (2) discloses: modifying a message to be transmitted during a session between a client and a server system to include a session identification flag and a session identifier corresponding to an originator of the session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system; and transmitting the message between the client and the server system; checking the transmitted message for the session identification flag. Pollutro(2) does not expressly teach reading the session identifier of the transmitted message to determine the originator of the message. However, at the time of applicant's original filing, the feature of using a session identifier to determine the originator of a message was well known in the art and would have been an obvious modification of Pollutro (2) as discloses by Williams. Williams discloses using a session identifier to determine the originator of a message [par. 64]. Therefore given Pollutro(2)'s use of session identifiers in communication packets, a person of ordinary skill in the art would have recognized the advantage of modifying Pollutor(2) to enhance network access control with the well known feature of using a session id to identify a user as disclosed by Williams.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-13 and 15-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Williams (US Patent Publication No. 2003/0005118) in view of Nguyen (US Patent No. 7,386,889).

5. As to claim 1, Williams teaches a method of Identifying the originator of a message transmitted between a client and a server system [par. 62], said method comprising the steps of: modifying (e.g., inserting) a message to be transmitted during a session between a client and a server system to include a session identification flag and a session identifier corresponding to an originator of the session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system (i.e., ...teaches the server may identify the client based upon the presented token [abstract] .... teaches service token, which is expected to be asserted by the client along with each request that the client sends to the protected server in order to identify the client to the protected server. The token also includes session information in some manner for allowing the protected server to identify the client's session context when a next request is received from the client within the

established session .... further teaches inserting session id into the token [par. 62]); transmitting the message between the client and the server system (i.e., ..teaches the client also sends a single-use service token [par. 63]); and reading (e.g., using) the session identifier of the transmitted message to determine the originator of the message (i.e., ..teaches the protected server uses the session ID in the service token to match the previously established session context with the client [par. 64]). The Examiner notes that William discloses that the session id is used to identify a user. See William paragraph 62. The Examiner contends that while William does not expressly disclose a flag field as part of the data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen, columns 4, 5 and 6. Furthermore the Examiner notes that Nguyen states that flag (0x05) may pertain to the user id (i.e., identification information for the originator). See Nguyen, column 5. Therefore given William's ability to designate that the session id is to be used as identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as a means to identify a particular action (e.g., command, attribute). With regards to applicant's claim limitation element of checking the transmitted message for the session identification flag, the Examiner contends that prior art reference Nguyen disclose a flag packet field. (See figure 2). Additionally, Nguyen describes reading (e.g., checking) the flag field during the session negotiation phase. Therefore given William's ability to designate that the session id is to be used as the identification means, a person of ordinary skill in the art would have recognized the

advantage of modifying William to enhance data packet communication by employing Nguyen's usage of a flag data packet field.

6. As to claim 2, William teaches a method where the step of modifying the message comprises the step of re-computing (e.g., generate) a control portion (e.g., data field) of the message to reflect the inclusion of the session identification flag and the session Identifier (e.g., session information) (i.e., ...teaches a session ID can be issued by the protected server and inserted in the service token; the session information is a session key contained in the data field of the cookie .... returns a newly generated service response message which comprises service token containing session information [par. 62]). The Examiner notes that William discloses that the session id is used to identify a user. See William paragraph 62. The Examiner contends that while William does not expressly disclose a flag field as part of the data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen columns 4, 5 and 6. Furthermore the Examiner notes that Nguyen states that the flag (0x05) pertains to a user id (i.e., identification information for the originator). See Nguyen column 4. Therefore given William's ability to designate that the session id is to be used as the identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as identification means.

7. As to claim 3, William teaches a method further comprising the steps of: removing the session identification flag and the session identifier from the transmitted message (i.e., ...teaches upon receiving the service token containing the session data, using the session data to determine if session data matches the previously established data [par. 64] ...note the William states that the session information is used thereby suggesting that the data was removed from the packet); and re-computing (e.g., refreshed) the control portion (e.g., service token) of the message to reflect the removal of the session identification flag and the session identifier (i.e., ...teaches additionally William asserts the client will receive a refreshed service token after session information has been used from the initial request. The refreshed service token a single use token suggesting that the session has been established [par. 66]). The Examiner notes that William discloses that the session id is used to identify a user. See William paragraph 62. The Examiner contends that while William does not expressly disclose a flag field as part of the data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen columns 4, 5 and 6. Furthermore the Examiner notes that Nguyen states that the flag (0x05) pertains to a user id (i.e., identification information for the originator). See Nguyen column 4. Therefore given William's ability to designate that the session id is to be used as identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag data packet field as means to identify a user. 5. As to claim 4, William teaches a method where the step of modifying the message (e.g.,

token) comprises appending the session identification flag and the session identifier at an end of the message (i.e., ...teaches that session information is included in the token (e.g., packet/message) [par. 62]) The Examiner notes that William discloses that the session id is used to identify a user. See William paragraph 62. The Examiner contends that while William does not expressly disclose a flag field as part of the data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen columns 4, 5 and 6. Furthermore the Examiner notes that Nguyen states that the flag (0x05) pertains to a user id (i.e., identification information for the originator). See Nguyen column 4. Therefore given William's ability to designate that the session id is to be used as identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag data packet field as means to identify a user.

8. As to claim 5, William teaches a method where the step of modifying the message further comprises at least one of changing the session identifier for each communication or changing the session identifier at a predetermined interval (i.e., ..teaches a single-use service token can be asserted only once by its owning entity, i.e. the entity with which the service token is associated. After a single-use service token has been used, it cannot be re-used without being refreshed or updated by its issuing entity so that it may be used again [par. 66]). 7. As to claim 6, William teaches a method of identifying the originator of a communication packet (i.e., ...teaches the server may

identify the client based upon the presented token [abstract]); transmitted between a client and a server in a client/server system (i.e., teaches the client also sends a single-use service token [par. 63]), said method :comprising the steps of: appending a session identifier and a security tag (i.e., data field) to the communication packet (i.e., cookie) (i.e., ...teaches session information is a session key contained in the data field of the cookie [par. 62]), the session identifier uniquely identifying the client in the client/server system (i.e., ... teaches server may identify the client based upon the presented token...further teaches the token comprises a session identifier [abstract]; authenticating (e.g., matched the session identifier using the security tag (e.g., session context) (i.e., ...teaches the session ID is subsequently matched to the client's session context when received by the protected server [par. 62]); if the appended session identifier is authenticated determining the originator of the transmitted communication packet based on the appended session identifier (i.e., teaches the protected server uses the session ID in the service token to match the previously established session context with the client, and the protected server processes the client's request [par. 64]). The Examiner contends that while William does not expressly disclose a flag field as part of the data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen columns 4, 5 and 6. The Examiner notes per applicant's specification paragraph 38, the flag field is also considered a security tag. See Nguyen columns 5 and 6, specifically Flag (0x09). In this instance the Examiner asserts that Nguyen's indication of encryption is equivalent to applicant's security tag (e.g. flag field) on the basis that the encryption of the data would

be a secure (e.g., security) means to transmit data. Therefore given William's ability to designate that the session id is to be used as the identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as a means to identify a particular communication security (e.g., encryption). 8. As to claim 7, William teaches a method further comprising the step of: establishing a common security tag in the client and server (i.e., ...teaches establishing a session id (e.g., security tag) between server and client [par. 62]), wherein the step of appending the session identifier includes appending the common security tag to the communication packet to be transmitted between the client and the server such 5 that a presence of the common security tag in the transmitted communication packet 6 indicates that the session identifier is authenticated (i.e., teaches inserting (i.e., appending) session id [par. 62]). The Examiner contends that while William does not expressly disclose a flag field as part of a data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen columns 4, 5 and 6. The Examiner notes per applicant's specification paragraph 38, the flag field is also considered a security tag. See Nguyen columns 5 and 6, specifically Flag (0x09). In this instance the Examiner asserts that Nguyen's indication of encryption is equivalent to applicant's security tag (e.g. flag field) on the basis that the encryption of the data would be a secure (e.g., security) means to transmit the data. Therefore given William's ability to designate that the session id is to be used as the identification means, a person of ordinary skill in the art would have recognized the advantage of

modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as a means to identify a particular communication security (e.g., encryption).

9. As to claim 8, William teaches a method further comprising the steps of: if the appended session identifier in the transmitted communication packet is authenticated, processing the transmitted communication packet according to predetermined rules for transmitted communication packets with authenticated session identifiers (i.e., teaches the protected server uses the session ID in the service token to match the previously established session context with the client, and the protected server processes the client's request [par. 64]); and if the appended session identifier in the transmitted communication packet is not authenticated, processing the transmitted communication packet according to predetermined rules for transmitted communication packets without authenticated session identifiers (i.e., ...teaches asserting a stale or invalid token would result in a failed operation and optionally other security measures [par. 66]).

10. As to claim 9, William teaches a method where the step of appending (e.g., inserting) the session identifier and the common security tag to the communication packet {par. 62] comprises the step of re-computing (e.g., generating) a control portion of the communication packet to be transmitted to reflect the inclusion of the common security tag and the session identifier (e.g., session information) (i.e., ...teaches a session ID can be issued by the protected server and inserted in the service token; the

session information is a session key contained in the data field of the cookie .... returns a newly generated service response message which comprises service token containing session information [par. 62]), the method further comprising the steps of: removing the session identification flag and the session identifier from the transmitted message (i.e., ...teaches upon receiving the service token containing the session data, using the session data to determine if session data matches the previously established data [par. 64] ...note the William states that the session information is used thereby suggesting that the data was removed from the packet); and re-computing (e.g., refreshed) the control portion (e.g., service token) of the message to reflect the removal of the session identification flag and the session identifier (i.e., ...teaches additionally William asserts the client will receive a refreshed service token after session information has been used from the initial request. The refreshed service token is a single use token suggesting that the session has been established [par. 66]). The Examiner contends that while William does not expressly disclose a flag field as part of a data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen columns 4, 5 and 6. The Examiner notes per applicant's specification paragraph 38, the flag field is also considered a security tag. See Nguyen columns 5 and 6, specifically Flag (0x09). In this instance the Examiner asserts that Nguyen's indication of encryption is equivalent to applicant's security tag (e.g. flag field) on the basis that the encryption of the data would be a secure (e.g., security) means to transmit the data. Therefore given William's ability to designate that the session id is to be used as the identification means, a person of ordinary skill in the

art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as a means to identify a particular communication security (e.g., encryption).

11. As to claim 10, William teaches a method further comprising the steps of: encrypting the communication packet to be transmitted after the step (i.e., teaches any information within a token may be encrypted to hide the information so as to limit the risk that it might be misappropriated [par. 50]); appending (i.e., inserting) the session identifier and the common security tag [par. 62]; and decrypting the transmitted communication packet prior to the steps of determining the originator of the transmitted communication packet (i.e., teaches encryption infrastructure (i.e., encryption/decryption) that might be used to support secure communication between the interacting entities [par. 78]), removing the common security tag and the session identifier (i.e., ...teaches upon receiving the service token containing the session data, using the session data to determine if session data matches the previously established data [par. 64] ...note the William states that the session information is used thereby suggesting that the data was removed from the packet), and re-computing (e.g., refresh) the control portion of the transmitted communication packet (i.e., ...teaches additionally William asserts the client will receive a refreshed service token after session information has been used from the initial request. The refreshed service token a single use token suggesting that the session has been established [par. 66]). The Examiner contends that while William does not expressly disclose a flag (e.g., security tag) field

as part of the data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen columns 4, 5 and 6. The Examiner notes per applicant's specification paragraph 38, the flag field is also considered a security tag. See Nguyen columns 5 and 6, specifically Flag (0x09). In this instance the Examiner asserts that Nguyen indication of encryption is equivalent to applicant's security tag (e.g. flag field) on the basis that the encryption of the data would be a secure (e.g., security) means to transmit the data. Therefore given William's ability to designate that the session id is to be used as the identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as a means to identify a particular communication security (e.g., encryption).

12. As to claim 11, Williams teaches a method further comprising the steps of: encrypting the communication packet to be transmitted prior to the step of appending the session identifier and the common security tag (i.e., teaches any information within a token may be encrypted to hide the information so as to limit the risk that it might be misappropriated [par. 50]); and decrypting the transmitted communication packet after the step of re- computing the control portion of the transmitted communication packet (i.e., teaches encryption infrastructure (i.e., encryption/decryption) that might be used to support secure communication between the interacting entities [par. 78]). The Examiner contends that while William does not expressly disclose a flag field (e.g. security tag) as part of the data packet structure, that prior art reference Nguyen disclosed that the flag

field may indicate data security related information (e.g. encryption). See Nguyen columns 5 and 6, specifically Flag (0x09). The Examiner notes per applicant's specification paragraph 38, the flag field is also considered a security tag. In this instance the Examiner asserts that Nguyen indication of encryption is equivalent to applicant's security tag (e.g. flag field) on the basis that the encryption of data would be a secure (e.g., security) means to transmit the data. Therefore given William's ability to designate that the session id is to be used as identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as a means to identify a particular communication security (e.g., encryption).

13. As to claim 12, Williams teaches a method further comprising the step of: setting a length of the common security tag (i.e., session information) greater than a predetermined length to reduce or substantially eliminate falsely authenticated session identifiers (i.e., teaches inserting the session information into a data field [par. 62]). The Examiner contends that while William does not expressly disclose a flag field (e.g. security tag) as part of the data packet structure, that prior art reference Nguyen disclosed that the flag field may indicate data security related information (e.g. encryption). See Nguyen columns 5 and 6, specifically Flag (0x09). The Examiner notes per applicant's specification paragraph 38, the flag field is also considered a security tag. In this instance the Examiner asserts that Nguyen indication of encryption is

equivalent to applicant's security tag (e.g. flag field) on the basis that the encryption of the data would be a secure (e.g., security) means to transmit the data. Therefore given William's ability to designate that the session id is to be used as identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as a means to identify a particular communication security (e.g., encryption).

14. As to claim 13, Williams teaches a method according where the length of the security tag is set to a length in the range of about 8 to 64 bits long [par. 62]. The Examiner contends that while William does not expressly disclose a flag field (e.g. security tag) as part of the data packet structure, that prior art reference Nguyen disclosed that the flag field may indicate data security related information (e.g. encryption). See Nguyen columns 5 and 6, specifically Flag (0x09).The Examiner notes per applicant's specification paragraph 38, the flag field is also considered a security tag. In this instance the Examiner asserts that Nguyen indication of encryption is equivalent to applicant's security tag (e.g. flag field) on the basis that the encryption of the data would be a secure (e.g., security) means to transmit the data. Therefore given William's ability to designate that the session id is to be used as identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to

include a flag field as a means to identify a particular communication security (e.g., encryption).

15. As to claim 14, (cancelled).

16. As to claim 15, William teaches a computer system for identifying the originator of a message [abstract], comprising: a server [fig. 2B]; and a client operationally connected to the server [fig. 2B], the client and server being configured to transmit one or more messages there between during a session [fig. 2B], each of the messages to be transmitted being modified by one of the client or the server to include a session identification flag and a session identifier (i.e., ...teaches the server may identify the client based upon the presented token [abstract] .... teaches service token, which is expected to be asserted by the client along with each request that the client sends to the protected server in order to identify the client to the protected server. The token also includes session information in some manner for allowing the protected server to identify the client's session context when a next request is received from the client within the established session .... further teaches inserting session information into the token [par. 62]); the client and server being further configured such that the modified message is transmitted (e.g., send) to the remaining one of the client and the server (i.e., teaches the client also sends a single-use service token [par. 63]); and the server to validate the session identifier (i.e., teaches the protected server uses the session ID in the service token to match the previously established session context with the client,

and the protected server processes the client's request [par. 64]); and if the session identifier is validated, the session identifier of the transmitted message is read to determine the originator of the transmitted message (i.e., teaches the CDC authenticates the client or user by processing the authentication data to determine whether or not the client or the user that is asserting itself has properly established its identity [par. 69]), the session identifier corresponding to an originator of a session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system (i.e., ..teaches the session id is used to identify the client [abstract]). The Examiner notes that William discloses that the session id is used to identify a user. See William paragraph 62. The Examiner contends that while William does not expressly disclose a flag field as part of the data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen columns 4, 5 and 6. Furthermore the Examiner notes that Nguyen states that flag (0x05) may pertain to the user id (i.e., identification information for the originator. See Nguyen column 5. Therefore given William's ability to designate that the session id is to be used as identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as a means to identify a particular action (e.g., command, attribute). With regards to applicant's claim limitation element of checking the transmitted message for the session identification flag, the Examiner contends that prior art reference Nguyen disclose a flag packet field. (See figure 2) Additionally Nguyen describes reading (e.g., checking) the

flag field during the session negotiation phase. Therefore given William's ability to designate that the session id is to be used as the identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's usage of a flag data field.
17. As to claim 16, William teaches a computer system further comprising a network gateway disposed operationally between the client and server and providing access to the server such that the server is remotely accessible by the client [fig. 2B].

17. As to claim 17, William teaches a computer system further comprising: an encrypting unit disposed on one side of the network gateway to encrypt the message to be transmitted (i.e., teaches any information within a token may be encrypted to hide the information so as to limit the risk that it might be misappropriated [par. 50]). 19. As to claim 18, William teaches a computer system further comprising: a decrypting unit disposed on another side of the network gateway to decrypt the transmitted message (i.e., teaches encryption infrastructure (i.e., encryption/decryption) that might be used to support secure communication between the interacting entities [par. 78]).

18. As to claim 19, William teaches a computer system where the message is processed sequentially such that either the message to be transmitted is encrypted by the encrypting unit and then modified and the transmitted message is read and then decrypted by the decrypting unit or the message to be transmitted is modified and then encrypted by the encrypting unit and the transmitted message is decrypted by the

decrypting unit and then read (i.e., teaches encryption infrastructure (i.e., encryption/decryption) that might be used to support secure communication between the interacting entities [par. 78]).

19. As to claim 20, William teaches a computer system where the network gateway includes a database to validate the session identifier by checking a user identifier (i.e., teaches the CDC authenticates the client or user by processing the authentication data to determine whether or not the client or the user that is asserting itself has properly established its identity [par. 69]), if the session identifier is not valid, the computer system forces the user to log in prior to accessing the server and if the session identifier is valid, the computer system retrieves an associated user identifier (i.e., ...teaches asserting a stale or invalid token would result in a failed operation and optionally other security measures [par. 66]) and the server processes the transmitted message (i.e., teaches the protected server uses the session ID in the service token to match the previously established session context with the client, and the protected server processes the client's request [par. 64]).

20. As to claim 21, Williams teaches computer readable carrier including computer program instructions which cause a computer system including at least a client and a server to implement a method of identifying the originator of a message transmitted between the client and the server (i.e., ..teaches establishing the identity of a client [abstract], said method comprising the steps of:, the session identifier being assigned

corresponding to the originator of the session on the server system and allowing the originator of the session to be uniquely identified among originators of sessions on the server system (i.e., ...teaches the server may identify the client based upon the presented token [abstract] .... teaches service token, which is expected to be asserted by the client along with each request that the client sends to the protected server in order to identify the client to the protected server. The token also includes session information in some manner for allowing the protected server to identify the client's session context when a next request is received from the client within the established session .... further teaches inserting session information into the token [par. 62]); re-computing (e.g., generating) a control portion of the message to reflect the inclusion of the session identification flag and the session identifier (e.g., session information) (i.e., ...teaches a session ID can be issued by the protected server and inserted in the service token; the session information is a session key contained in the data field of the cookie .... returns a newly generated service response message which comprises service token containing session information [par. 62]); transmitting the message between the client and the server (i.e., teaches the client also sends a single-use service token [par. 63]);

reading (e.g., using) the session identifier of the transmitted message to determine the originator of the message (i.e., ..teaches the protected server uses the session ID in the service token to match the previously established session context with the client [par. 64]); removing the session identification flag and the session identifier from the transmitted message (i.e., ...teaches upon receiving the service token

containing the session data, using the session data to determine if session data matches the previously established data [par. 64] ...note the William states that the session information is used thereby suggesting that the data was removed from the packet); and re-computing (e.g., refreshed) the control portion (e.g., service token) of the message to reflect the removal of the session identification flag and the session identifier (i.e., ...teaches additionally William asserts the client will receive a refreshed service token after session information has been used from the initial request. The refreshed service token is a single use token suggesting that the session has been established [par. 66]). The Examiner notes that William discloses that the session id is used to identify a user. See William paragraph 62. The Examiner contends that while William does not expressly disclose a flag field as part of the data packet structure, that prior art reference Nguyen disclosed a packet structure comprising both a flag field and a session id. See Nguyen columns 4, 5 and 6. Furthermore the Examiner notes that Nguyen states that flag (0x05) may pertain to the user id (i.e., identification information for the originator. See Nguyen column 5. Therefore given William's ability to designate that the session id is to be used as identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's capability to include a flag field as a means to identify a particular action (e.g., command, attribute). With regards to applicant's claim limitation element of checking the transmitted message for the session identification flag, the Examiner contends that prior art reference Nguyen disclose a flag packet field. (See figure 2) Additionally Nguyen describes reading (e.g., checking) the flag field

during the session negotiation phase. Therefore given William's ability to designate that the session id is to be used as the identification means, a person of ordinary skill in the art would have recognized the advantage of modifying William to enhance data packet communication by employing Nguyen's usage of a flag data packet field.

Response to Arguments

Examiner Remarks - Double Patenting Rejection

The Examiner maintains Double Patent Rejection. Once a formal Terminal Disclaimer is filed and approved the Examiner will withdraws the Double Patent Rejection.

Examiner Remarks – 35 U.S.C. 101

The Examiner noted in office action mailed on 2/11/2011 that applicant's specification explicitly states that the system may be implemented in a number of “mediums”. The applicant further describes that such a "medium" includes a ‘computer readable carrier" for which the applicant adds includes waves. See applicant's paragraph 36 and 46.

The Examiner respectfully contends that subject matter consisting of waves are considered to be non-statutory subject matter. Therefore, the Examiner submits that applicant’s disclosure of "mediums" of the system consisting of "computer readable carrier" for which is described to comprise of waves is considered to be non-statutory subject matter. As such the Examiner maintains rejection made under 35 U.S.C. 101.

Examiner Remarks – 35 U.S.C. 103(a)

Examiner Remarks - Claims 1-13 and 15-21 Unpatentable over Williams and Nguyen

Applicant argues:

> "The combination of Williams and Nguyen fails to teach or suggest modifying a message to include a session identification flag and a session identifier. The Examiner cites Williams'"

The Examiner notes that applicant's paragraph 23 reads: "If the communication/message is sent from a client to a server, the message may be modified on the client side (i.e., at the client or on the side of the network gateway of the client) to add a session identification flag and a session identifier at the end of the message". Additionally the Examiner notes paragraph 23 of applicant's original disclosure recites the following: "If the communication/message is sent from a client to a server". The Examiner contends that applicant's "communication/message" can be properly construed/interpretation as applicant's message is equivalent and can be any communication between server and client. This interpretation is further justified by applicant's usage of the term packet as it relates to communication/messaging between the server and client in applicant's paragraph 41.

In response to the argument presented above by the applicant, the Examiner notes in this instance William's paragraph 62. The Examiner contends paragraph 62 discloses "…a session ID can be issued by the protected server and inserted in the service token". The Examiner contends William's token is representative of communication between server and client. As noted earlier the Examiner established that applicant's message is essentially equivalent to communication between a server and client. The Examiner further contends that the "insert' process element as disclosed by Williams'

can be properly construed as a modification. The Examiner notes William states that a service token is generated and as part of the session establishment between a server and client a "session id" is inserted into the service token. Additionally the Examiner notes that the ordinary meaning of the word “insert” is the process of adding. Therefore the Examiner notes that William’s teachings properly convey the capability to modify a communication between a server and client with a session id.

With regards to applicant’s flag element, the Examiner notes that the applicant disclosed in paragraph 41 of their original disclosure the following: “it is determined whether a flag is added that indicates that the message contains an embedded identifier”. The Examiner contends that applicant’s usage of the flag is to merely indicate the presences of specific data in the communication data packet. The Examiner respectfully notes that Nguyen’s teachings disclosed the use of flags for particularly indicating packet related data.

The Examiner respectfully adds that the teachings William\’s clearly established that prior to applicant’s original filing date that the capability of inserting “session id” data in communication packets between a server and client and subsequently using the session id data for verification purpose was known. The Examiner additionally notes that William's original disclosure disclosed processing incoming packet communication. The Examiner notes that the teachings of Nguyen disclosed using a flag as part of the packet structures as means to determine specific content of incoming packets. The

Examiner respectfully contends that modifying William with Nguyen's capability to process incoming packet based on flag data would inherently enhance William's incoming packet processing process.

Examiner Remarks - B. Independent Claim 6 Un-Patentable Over Williams and Nguyen

Applicant's argues:

> "The Examiner appears to rely on his arguments from claim 1 for claim 6 although claim 6 had different claim elements. Nevertheless, neither Williams nor Nguyen authenticate the session identifier appended to the packet using the security tag appended to the packet. Williams does not use one item of the message to authenticate another item in the same message. Nowhere in Williams does Williams describe using a data field of the message to authenticate a value of another data filed in the same message."

The Examiner notes in this instance that the applicant discloses in paragraph 41 of their original disclosure the following: "it is determined whether a flag is added that indicates that the message contains an embedded identifier". The Examiner contends that applicant's usage of a flag is to merely indicate the presences of specific data in the communication data packet.

The Examiner respectfully notes that applicant's flag data does not authenticate another data field as argued above, however simply applicant's flag as stated by applicant in applicant's original disclosure paragraph 41 is merely used to identify the presence of a specific packet related data (e.g., session id) within the received communication packet. The Examiner notes Nguyen teachings specifically disclosed using flag data in data

packet structures and making a determination relative to the packet on the basis of the flag related data pertaining to specific data packet within.

In response to the argument presented above by the applicant, the Examiner notes in this instance William's paragraph 62. The Examiner contends paragraph 62 discloses "…a session ID can be issued by the protected server and inserted in the service token". The Examiner contends William's token is representative of communication between server and client. As noted earlier the Examiner established that applicant's message is essentially equivalent to communication between a server and client. The Examiner further contends that the "insert' process element as disclosed by Williams' can be properly construed as a modification. The Examiner notes William states that a service token is generated and as part of the session establishment between a server and client a "session id" is inserted into the service token. Additionally the Examiner notes that the ordinary meaning of the word "insert" is the process of adding. Therefore the Examiner notes that William's teachings properly convey the capability to modify a communication between a server and client with a session id. The Examiner notes with regards to applicant's use of the session id for authentication purposes, the Examiner notes that William's discloses in paragraph 62 using the "session id" as means to verify (e.g. authenticate) communication with the client.

With regards to applicant's flag element, the Examiner notes that the applicant disclosed in paragraph 41 of their original disclosure the following: "it is determined

whether a flag is added that indicates that the message contains an embedded identifier". The Examiner contends that applicant's usage of the flag is to merely indicate the presences of specific data in the communication data packet. The Examiner respectfully notes that Nguyen's teachings disclosed the use of flags for particularly indicating packet related data.

The Examiner further notes modifying William's teachings with those of Nguyen would have rendered an obvious communication packet processing enhancement over William's present system. William expressly taught making determinations as it relates to incoming communication packets in paragraphs 73 and 74. The Examiner contends by incorporating Nguyen's system capability of utilizing and processing flag related data, William's communication packet processing would be more efficient allowing processing of the incoming packet to be contingent on the flag value.

Examiner Remarks - C. Independent Claim 15

Un-Patentable Over Williams and Nguyen

Applicant argues:

> "Neither Williams nor Nguyen teach or suggest checking the session identification flag of the transmitted message to validate the session identifier. "

First the Examiner respectfully notes that applicant's flag does not authenticate another data field as argued above. Applicant's flag as stated by applicant in applicant's original

disclosure paragraph 41 is merely used to identify the presence of a specific packet related data (e.g., session id) within the received communication packet.

Secondly the Examiner notes that while William's teachings do not expressly teach the use of a flag to process an incoming packet, William's teachings certainly discloses processing incoming data packets. As such it would be obvious to enhance the process speed of processing incoming packets by adding a flag and basing the incoming packet processing contingent on the value of the flag. The Examiner contends that the packet processor can be programmed to analyze for a specific flag value in the incoming packet. If the incoming packet contains the specific value than the packet processor can act accordingly. The Examiner respectfully notes that such an enhancement would come as a result of modifying William's teachings with Nguyen's capability to use flag related data to indicated packet contents.

Additionally the Examiner notes that Nguyen teachings when the incoming packet is received, the flag related data is checked. This flag related data would indicated the nature of the packet's content (i.e., validate the session identifier). The packet would than be processed accordingly.

Examiner Remarks - D. Independent Claim 21 Patentable Over Williams and Nguyen

Applicant argues:

> “Neither Williams nor Nguyen teach or suggest re-computing a control portion of the message to reflect the inclusion or removal of the session identification flag and the session identifier”.

The Examiner notes applicant's usage of the term "or" renders applicant’s statement in alternative form. As such with regards to applicant's claim limitation of " a control portion of the message to reflect the inclusion of the session identification flag and the session identifier”, the Examiner notes that the teachings of Nguyen discloses packets with the inclusion of a flag field. With regard to applicant's "re-compute" claim element the Examiner notes that paragraph 38 of applicant's original disclosure suggest that the process of "re-computing" simply involves inserting data into a packet structure. As such the Examiner notes that William's discloses in paragraph 62 the capability of inserting new data into a data packet.

Additionally the Examiner notes that applicant's original disclosure does not suggest any deviation from the implementation of the standard OSI model. The Examiner notes that those skilled in the art would recognize that there are standard TCP packet sizes as part of a TCP communication protocol and that any deviation from the standard allowable packet sizes and fields would not adhere to proper communication TCP communication. As such applicant’s data packet would have to have the available data field space for the inclusion of new data. Therefore the Examiner respectfully contends that applicant’s

“re-computing” claim element must therefore only be a data insertion process that is constrained by the available data field space in the packet and nothing more.

With regards to applicant’s argument of "..., Williams and Nguyen cannot have a session identification flag, a session identifier and a control portion in the same message”, again the Examiner notes that applicant's original disclosure does not suggest any deviation from the implementation of the standard OSI model. As such the Examiner notes that those skilled in the art would recognize that there are standard TCP packet sizes as part of a TCP communication protocol and that any deviation from the standard allowable packet sizes and fields would not adhere to proper communication TCP communication. Therefore applicant’s data packet would have to have the available data field space for the inclusion of new data. The Examiner respectfully contends that both William and Nguyen teaching adhere to the OSI model and communication protocol there within.

With regards to applicant’s remarks or “This simply would not equate to re-computing a control portion of the message to reflect the inclusion of the session identification flag and the session identifier in the message”, the Examiner notes that per the illustration of applicant’s figure 3, the session id and session flag is not part of the control portion of the packet. Based on the illustration in figure 3, the Examiner does not follow applicant's argument. Again the Examiner notes that applicant's original disclosure does not suggest any deviation from the implementation of the standard OSI model. The Examiner notes that those skilled in the art would recognize that there are standard

TCP packet sizes as part of a TCP communication protocol and that any deviation from the standard allowable packet sizes and fields would not adhere to proper communication TCP communication. As such applicant's data packet would have to have the available data field space for the inclusion of new data. Therefore the Examiner respectfully contends that applicant's "re-computing" claim element must therefore only be a data insertion process that is constrained by the available data field space in the packet and nothing more. The Examiner further submits based on the illustration of figure 3 that the Examiner is confused on what is illustrated in the figure 3 and applicant's arguments reciting that the session id and session flag is part of the control information and that the control information is re-computed to re-computing a control portion of the message to reflect the inclusion or removal of the session identification flag and the session identifier. See page 8 of applicant remarks submitted on 5/11/2011. The Examiner respectfully contends that Figure 3 explicitly illustrates that the session id and session flag is not part of the control information/data.

Again the Examiner notes that applicant's original disclosure does not suggest any deviation from the implementation of the standard OSI model. The Examiner notes that those skilled in the art would recognize that there are standard TCP packet sizes and fields as part of a TCP communication protocol and that any deviation from the standard allowable packet sizes and fields would not adhere to proper communication TCP communication.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Flynn Nathan can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431